# Near-Collision Attack on the Compression Function of Dynamic SHA2

Hongbo Yu[1] and Xiaoyun Wang[2]*

[1] Tsinghua University, Beijing 100084, China
`yuhongbo@tsinghua.edu.cn`
[2] Tsinghua University and Shandong University, China
`xiaoyunwang@tsinghua.edu.cn, xywang@sdu.edu.cn`

**Abstract.** In this paper, we present a near-collision attack on the compression functions of Dynamic SHA2 for all the output sizes. For the Dynamic SHA2-224/256, the complexity is about $2^{45}$ operations and for the Dynamic SHA2-384/512, the complexity is about $2^{75}$.

## 1 Description of Dynamic SHA2

The Dynamic SHA-2 [1] is an iteration cryptographic hash function family which is built with the design components from SHA-2 family [2]. It provides the message digests of 224, 256, 384 and 512 bits. The fundamental building block of Dynamic SHA2-256 (Dynamic SHA2-512) is the compression function that takes 256-bit (512-bit) chaining value and 512-bit (1024-bit) message block and outputs a new 256-bit (512-bit) chaining value. For our purpose attack, we only describe the compression function of Dynamic SHA2 which includes three iterative parts. The first part includes only one round and mixs all the message words one time; the second iterative part includes 9 blank rounds and no message words are mixed, so it has no effect on our attack and we can neglect to describe it; and the third part includes 7 rounds and mixs the message words 7 times. The compression function of the Dynamic SHA2 can be described are as follows:

1. Input the 512-bit (resp. 1024-bit) message $W = (w_0, w_1, ..., w_{15})$, and initialize the eight chaining variables ($a$, $b$, $c$, $d$, $e$, $f$, $g$, $h$) with the $(i-1)^{th}$ hash value $(a_0, b_0, c_0, d_0, e_0, f_0, g_0, h_0)$.

2. Step update:
   - The first iterative part
     $COMP(a, b, c, d, e, f, g, h, w_0, w_1, w_2, w_3, w_4, w_5, w_6, w_7, 0)$
     $COMP(a, b, c, d, e, f, g, h, w_8, w_9, w_{10}, w_{11}, w_{12}, w_{13}, w_{14}, w_{15}, 0)$
   - The second iterative part (No message words are mixed, we neglect to describe it).

* Supported by 973 Project(No.2007CB807902), 863 Project(No.2006AA01Z420) and the National Natural Science Foundation of China(NSFC Grant No.60803125)

- The third iterative part

```
For $t$=1 to 7
{
$COMP(a, b, c, d, e, f, g, h, w_0, w_1, w_2, w_3, w_4, w_5, w_6, w_7, 0)$
$COMP(a, b, c, d, e, f, g, h, w_8, w_9, w_{10}, w_{11}, w_{12}, w_{13}, w_{14}, w_{15}, 0)$
}
```

3. Output:
   $a = a + a_0, b = b + b_0, \; c = c + c_0, \; d = d + d_0$
   $e = e + e_0, \; f = f + f_0, g = g + g_0, h = h + h_0$

The function $COMP(a, b, c, d, e, f, g, h, w(0), w(1), ..., w(7), t)$ for Dynamic SHA2 are defined in Table 1.

The notation $ROTR(x, n)$ denote the 32-bit (or 64-bit) word $x$ circular right shifts by $n$ bits and $SHR^n(x)$ denote $x$ right shifts by $n$ bits. The Boolean function $G(x, y, z, t)$ is defined as follows:

$$G(x, y, z, t) = \begin{cases} x \oplus y \oplus z & t = 0 \\ (x \wedge y) \oplus z & t = 1 \\ (\neg(x \vee z)) \wedge (x \vee (y \oplus z)) & t = 2 \\ (\neg(x \vee (y \oplus z))) \vee (x \wedge \neg z) & t = 3 \end{cases}$$

It easy to deduced the properties of $G_t = G(x, y, z, t)$ which is useful for our attack (See Table 2) .

## 2 The Near-Collision Attack on the Compression Function of Dynamic SHA2-224/256

The compression function Dynamic SHA2-224/256 is composed of eight rounds and each round can be decomposed four sub-steps. In order to facilitate our analysis, we list the detail step operations of the Dynamic SHA2-256 in Table 4 and it includes 32 steps altogether.

Following the notations in the breaking MD5 and SHA-1 [3, 4], let $x' = x[i]$ denote that $x$ and $x'$ is different only in the $i$-th bit and the other 31 bits are the same, $x_i$ denote the $i - th$ bit of the message word $x$ where the least significant bit is the 1-th bit, and the $x_{i \sim j}$ denote the value of $x$ from the $i - th$ bit to the $j - th$ bit, i.e., $x_{i \sim j} = x_i + 2x_{i+1} + 2^2 x_{i+2} + ... + 2^{j-i} x_j$.

Let the input chaining variable difference

$$(\Delta a_0, \Delta b_0, \Delta c_0, \Delta d_0, \Delta e_0, \Delta f_0, \Delta g_0, \Delta h_0) = (0, 0, 0, 0, 0, 0, 0, 2^{31}),$$

and the input message difference $\Delta W = W' - W = (\Delta w_0, \Delta w_1, ..., \Delta w_{15})$, where $\Delta w_1 = 2^{31}$ and $\Delta w_i = 0$ when $i \neq 1$.

The basic idea of our attack is to control the differences of the chaining variables only appearing at the most significant bit (32-*th* bit) by choosing the corresponding bits of the message words. The differential path in the Table 4 can be deduced as follows:

**Table 1.** Function $COMP$ for Dynamic SHA2.

| | |
|---|---|
| Dynamic SHA2-224/256 | $T = ROTR((((((((a \oplus b) + c) \oplus d) + e) \oplus f) + g) \oplus h), w(t) \wedge 31)$<br>$h = g$<br>$g = ROTR(f, SHR^{5}(w(t)) \wedge 31)$<br>$f = e + w((t + 3) \wedge 7)$<br>$e = ROTR(d, SHR^{10}(w(t)) \wedge 31)$<br>$d = G(a, b, c, SHR^{30}(w(t))) + w((t + 2) \wedge 7)$<br>$c = b$<br>$b = a$<br>$a = T + w((t + 1) \wedge 7)$<br>$T = ROTR((((((((a \oplus b) + c) \oplus d) + e) \oplus f) + g) \oplus h), SHR^{15}(w(t)) \wedge 31)$<br>$h = g + w((t + 7) \wedge 7)$<br>$g = ROTR(f, SHR^{20}(w(t)) \wedge 31)$<br>$f = e + w((t + 6) \wedge 7)$<br>$e = ROTR(d, SHR^{25}(w(t)) \wedge 31)$<br>$d = G(a, b, c, t \wedge 3) + w((t + 5) \wedge 7)$<br>$c = b + w(t)$<br>$b = a$<br>$a = T + w((t + 4) \wedge 7)$ |
| Dynamic SHA2-384/512 | $T = ROTR((((((((a \oplus b) + c) \oplus d) + e) \oplus f) + g) \oplus h), w(t) \wedge 63)$<br>$h = g$<br>$g = ROTR(f, SHR^{6}(w(t)) \wedge 63)$<br>$f = ROTR(e, SHR^{12}(w(t)) \wedge 63) + w((t + 3) \wedge 7)$<br>$e = ROTR(d, SHR^{18}(w(t)) \wedge 63)$<br>$d = G(a, b, c, SHR^{62}(w(t))) + w((t + 2) \wedge 7)$<br>$c = ROTR(b, SHR^{24}(w(t)) \wedge 63)$<br>$b = a$<br>$a = T + w((t + 1) \wedge 7)$<br>$T = ROTR((((((((a \oplus b) + c) \oplus d) + e) \oplus f) + g) \oplus h), SHR^{30}(w(t)) \wedge 63)$<br>$h = g + w((t + 7) \wedge 7)$<br>$g = ROTR(f, SHR^{36}(w(t)) \wedge 63)$<br>$f = ROTR(e, SHR^{42}(w(t)) \wedge 63) + w((t + 6) \wedge 7)$<br>$e = ROTR(d, SHR^{48}(w(t)) \wedge 63)$<br>$d = G(a, b, c, SHR^{60}(w(t)) \wedge 3) + w((t + 5) \wedge 7)$<br>$c = b + w(t)$<br>$b = ROTR(a, SHR^{54}(w(t)) \wedge 63)$<br>$a = T + w((t + 4) \wedge 7)$ |

**Table 2.** Properties of the Boolean function $G_0$, $G_1$, $G_2$ and $G_3$.

| $\Delta a$ | $\Delta b$ | $\Delta c$ | $\Delta G_0 = 0$ | $\Delta G_0 = 1$ | $\Delta G_1 = 0$ | $\Delta G_1 = 1$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | – | 1 | – |
| 0 | 0 | 1 | – | 1 | – | 1 |
| 0 | 1 | 0 | – | 1 | $a = 0$ | $a = 1$ |
| 0 | 1 | 1 | 1 | – | $a = 1$ | $a = 0$ |
| 1 | 0 | 0 | – | 1 | $b = 0$ | $b = 1$ |
| 1 | 0 | 1 | 1 | – | $b = 1$ | $b = 0$ |
| 1 | 1 | 0 | 1 | – | $a = b \oplus 1$ | $a = b$ |
| 1 | 1 | 1 | – | 1 | $b = 1$ | $b = 0$ |
| $\Delta a$ | $\Delta b$ | $\Delta c$ | $\Delta G_2 = 0$ | $\Delta G_2 = 1$ | $\Delta G_3 = 0$ | $\Delta G_3 = 1$ |
| 0 | 0 | 0 | 1 | – | 1 | – |
| 0 | 0 | 1 | – | 1 | – | 1 |
| 0 | 1 | 0 | $a = 0$ | $a = 1$ | $a = 1$ | $a = 0$ |
| 0 | 1 | 1 | $a = 1$ | $a = 0$ | $a = 0$ | $a = 1$ |
| 1 | 0 | 0 | $b = 1$ | $b = 0$ | $b = 0$ | $b = 1$ |
| 1 | 0 | 1 | $b = 0$ | $b = 1$ | $b = 1$ | $b = 0$ |
| 1 | 1 | 0 | $a = b$ | $a = b \oplus 1$ | $a = b$ | $a = b \oplus 1$ |
| 1 | 1 | 1 | $a = b \oplus 1$ | $a = b$ | $a = b$ | $a = b \oplus 1$ |

1. In the round 1 ($t$=0), we set $w_{0,1\sim5} = 0$, then the number of the rotation shift in $T_1$ is zero, so $\Delta T_1 = 2^{31}$, i.e., $T'_1 = T_1[32]$. Because $\Delta w_1 = 2^{31}$, then $\Delta a_1 = \Delta T_1 + \Delta w_1 = 2^{31} + 2^{31} = 0$. So after the first round (steps 1 to 4), the outputs of the message $W$ and $W'$ consist of a collision.

   **Because there is no message word mixed in the second iteration part, the outputs of the messages $W$ and $W'$ after the second iteration also consist of a collision.**
2. In the round 2 ($t = 1$),
   - Step 5: the difference $w_1[32]$ will result that the different $G$ functions are used in the computations of $d_5$ and $d'_5$. From the truth table of the Boolean functions $G$, it's easy to known that the probabilities $Pr(G(x, y, z, 0) = G(x, y, z, 2)) = 2^{-2}$ and $Pr(G(x, y, z, 1) = G(x, y, z, 3)) = 1/2$ where $x$, $y$ and $z$ are all the single bits. So when we set $w_{1,31} = 1$, we get

     $$\begin{aligned} & Pr(d_5 = d'_5) \\ & Pr(G(a_4, b_4, c_4, SHR^{30}(w_1)) = G(a_4, b_4, c_4, SHR^{30}(w_1[32])) \\ = {} & Pr(G(a_4, b_4, c_4, 1) = G(a_4, b_4, c_4, 3)) \\ = {} & 2^{-32}. \end{aligned}$$

   - Step 6: the difference $w_1[32]$ will result to $c'_6 = c_6[32]$.
   - Step 7: Set $w_{9,1\sim5} = 0$, then shift number in $T_7$ is $w_9 \wedge 31 = 0$. So $\Delta T_7 = \Delta c_6 = 2^{31}$, i.e., $T_7 = T'_7[32]$, then $a'_7 = a_7[32]$. According to the properties of the $G$ functions, the probability that $G(x, y, 0, t) = G(x, y, 1, t)$

always equals to zero no matter the values of $t$. So we get $d'_7 = d_7[32]$.

- Step 8: Because $\Delta T_8 = \Delta a_7 + \Delta d_7 = 0$, so $\Delta a_8 = 0$, and $\Delta b_8 = \Delta a_7 = 2^{31}$. According to property of the function $G(x, y, z, 1)$, $Pr(G(a_7, b_7, c_7, 1) = G(a_7[32], b_7, c_7, 1) = 1/2$, i.e., $d'_8 = d_8$ when $b_{7,32} = 0$. Set $w_{9,26\sim30} = 0$, then $\Delta e_8 = \Delta d_7 = 2^{31}$.

Overall, after this round, the probability that the output difference in chaining variables

$$(\Delta a_8, \Delta b_8, \Delta c_8, \Delta d_8, \Delta e_8, \Delta f_8, \Delta g_8, \Delta h_8) = (0, 2^{31}, 0, 0, 2^{31}, 0, 0, 0)$$

is equal to $2^{-33}$ when we set the message values $w_{1,31} = 1$, $w_{9,1\sim5} = 0$ and $w_{9,26\sim30} = 0$.

3. In round 3 ($t = 2$), we set the message values $w_{2,31} = 1$, $w_{2,32} = 0$, $w_{2,21\sim25} = 0$, $w_{10,1\sim5} = 0$ and $w_{10,11\sim20} = 0$. Then the probability for the output difference in chaining variables

$$(\Delta a_{12}, \Delta b_{12}, \Delta c_{12}, \Delta d_{12}, \Delta e_{12}, \Delta f_{12}, \Delta g_{12}, \Delta h_{12}) = (2^{31}, 2^{31}, 0, 0, 0, 2^{31}, 0, 0)$$

is equal to $2^{-2}$. The detail differential characteristic can be refer to Table 4.

4. In round 4 ($t = 3$), we set the message values $w_{3,31\sim32} = 0$, $w_{3,1\sim10} = 0$, $w_{11,5\sim10} = 0$ and $w_{11,31\sim32} = 0$. Then the probability for the output difference in chaining variables

$$(\Delta a_{16}, \Delta b_{16}, \Delta c_{16}, \Delta d_{16}, \Delta e_{16}, \Delta f_{16}, \Delta g_{16}, \Delta h_{16}) = (0, 0, 0, 2^{31}, 0, 0, 0, 2^{31})$$

is equal to $1/2$.

5. In round 5 ($t = 4$), we set the message values $w_{4,11\sim20} = 0$, $w_{12,1\sim15} = 0$ and $w_{12,31} = 1$. Then the probability for the output difference in chaining variables

$$(\Delta a_{20}, \Delta b_{20}, \Delta c_{20}, \Delta d_{20}, \Delta e_{20}, \Delta f_{20}, \Delta g_{20}, \Delta h_{20}) = (0, 2^{31}, 2^{31}, 0, 0, 2^{31}, 0, 2^{31})$$

is equal to $1/2$.

6. In round 6 ($t = 5$), we set the message values $w_{5,31\sim32} = 0$, $w_{5,6\sim10} = 0$, $w_{13,31} = 1$, $w_{13,1\sim5} = 0$ and $w_{13,11\sim20} = 0$. Then the probability for the output difference in chaining variables

$$(\Delta a_{24}, \Delta b_{24}, \Delta c_{24}, \Delta d_{24}, \Delta e_{24}, \Delta f_{24}, \Delta g_{24}, \Delta h_{24}) = (2^{31}, 2^{31}, 2^{31}, 0, 0, 2^{31}, 0, 0)$$

is equal to $1/4$.

7. In round 7 ($t = 6$), we set the message values $w_{6,31} = 1$, $w_{6,6\sim10} = 0$, $w_{6,21\sim25} = 0$, $w_{14,1\sim5} = 0$, $w_{14,16\sim20} = 0$, $w_{14,26\sim30} = 0$. Then the probability for the output difference in chaining variables
$$(\Delta a_{28}, \Delta b_{28}, \Delta c_{28}, \Delta d_{28}, \Delta e_{28}, \Delta f_{28}, \Delta g_{28}, \Delta h_{28}) = (2^{31}, 2^{31}, 0, 0, 2^{31}, 0, 0, 0)$$
is equal to $2^{-3}$.

8. In round 8 ($t = 7$), we set the message values $w_{7,31} = 1$, $w_{7,32} = 0$ $w_{7,1\sim5} = 0$, $w_{7,21\sim25} = 0$, $w_{15,31\sim32} = 0$, $w_{15,1\sim5} = 0$, $w_{15,16\sim20} = 0$. Then the probability for the output difference in chaining variables
$$(\Delta a_{32}, \Delta b_{32}, \Delta c_{32}, \Delta d_{32}, \Delta e_{32}, \Delta f_{32}, \Delta g_{32}, \Delta h_{32}) = (2^{31}, 2^{31}, 0, 0, 0, 0, 0, 2^{31})$$
is equal to $2^{-3}$.

So for the Dynamic SHA2-256, if we fix the following message bits (See Table 3 for message $W$, then $W$ and $W'$ will obey the differential path in Table 4 with probability $2^{-45}$.

**Table 3.** The fixed message bits for Dynamic SHA2-224/256.

| | | | |
|---|---|---|---|
| $w_{0,1\sim5} = 0$ | $w_{1,31} = 1$ | $w_{2,21\sim25} = 0$,<br>$w_{2,31} = 1$,<br>$w_{2,32} = 0$ | $w_{3,1\sim10} = 0$,<br>$w_{3,31\sim32} = 0$ |
| $w_{4,11\sim20} = 0$ | $w_{5,6\sim10} = 0$,<br>$w_{5,31\sim32} = 0$ | $w_{6,6\sim10} = 0$,<br>$w_{6,21\sim25} = 0$,<br>$w_{6,31} = 1$ | $w_{7,1\sim5} = 0$,<br>$w_{7,21\sim25} = 0$,<br>$w_{7,31} = 1$,<br>$w_{7,32} = 0$ |
| | $w_{9,1\sim5} = 0$,<br>$w_{9,26\sim30} = 0$ | $w_{10,1\sim5} = 0$,<br>$w_{10,11\sim20} = 0$ | $w_{11,5\sim10} = 0$,<br>$w_{11,31\sim32} = 0$ |
| $w_{12,1\sim15} = 0$,<br>$w_{12,31} = 0$ | $w_{13,1\sim5} = 0$,<br>$w_{13,11\sim20} = 0$,<br>$w_{13,31} = 1$ | $w_{14,1\sim5} = 0$,<br>$w_{14,16\sim20} = 0$,<br>$w_{14,26\sim30} = 0$ | $w_{15,1\sim5} = 0$,<br>$w_{15,16\sim20} = 0$,<br>$w_{15,31\sim32} = 0$ |

## 3 The Near-Collision Attack on the Compression Function of Dynamic SHA2-384/512

For the compression function of Dynamic SHA2-384/512, it's easy to get a similar differential path as in Table 4 from the input difference $(0, 0, 0, 0, 0, 0, 0, 2^{63})$ to the output difference $(2^{63}, 2^{63}, 0, 0, 0, 0, 0, 2^{63})$ with probability $2^{-75}$. We select the message difference $\Delta w_1 = 2^{63}$ and $\Delta w_i = 0$ when $i \neq 1$. The message bits that need to be fixed to keep the diffusion only in the most significant bit (the 64-*th* bit) are listed in Table 3:

**Table 4.** The fixed message bits for Dynamic SHA2-224/256.

| |
|---|
| $w_{0,1\sim 6} = 0$ |
| $w_{1,63} = 1$ |
| $w_{2,13\sim 18} = 0$, $w_{2,25\sim 30} = 0$, $w_{2,37\sim 42} = 0$, $w_{2,63} = 1$, $w_{2,64} = 0$ |
| $w_{3,1\sim 12} = 0$, $w_{3,25\sim 30} = 0$, $w_{3,55\sim 60} = 0$, $w_{3,62} = 1$, $w_{3,63\sim 64} = 0$ |
| $w_{4,19\sim 24} = 0$ $w_{4,31\sim 36} = 0$, $w_{4,43\sim 48} = 0$ |
| $w_{5,7\sim 12} = 0$, $w_{5,25\sim 30} = 0$, $w_{5,63\sim 64} = 0$ |
| $w_{6,7\sim 12} = 0$, $w_{6,25\sim 30} = 0$, $w_{6,37\sim 42} = 0$, $w_{6,61\sim 62} = 0$, $w_{6,64} = 1$ |
| $w_{7,1\sim 6} = 0$, $w_{7,13\sim 18} = 0$, $w_{7,25\sim 30} = 0$, $w_{7,55\sim 60} = 0$, $w_{7,61} = 1$, $w_{7,62} = 0$, $w_{7,63} = 1$, $w_{7,64} = 0$ |
| $w_{9,1\sim 6} = 0$, $w_{9,49\sim 60} = 0$, $w_{9,61} = 1$ |
| $w_{10,1\sim 6} = 0$, $w_{10,19\sim 24} = 0$, $w_{10,31\sim 36} = 0$, $w_{10,43\sim 48} = 0$, $w_{10,55\sim 60} = 0$, $w_{10,61} = 1$ |
| $w_{11,7\sim 12} = 0$, $w_{11,25\sim 30} = 0$, $w_{11,63\sim 64} = 0$ |
| $w_{12,1\sim 12} = 0$, $w_{12,19\sim 24} = 0$, $w_{12,43\sim 48} = 0$, $w_{12,55\sim 62} = 0$, $w_{12,63} = 1$, $w_{12,64} = 0$ |
| $w_{13,1\sim 6} = 0$, $w_{13,19\sim 24} = 0$, $w_{13,31\sim 36} = 0$, $w_{13,43\sim 48} = 0$, $w_{13,55\sim 60} = 0$, $w_{13,61\sim 62} = 0$, $w_{13,63} = 1$ |
| $w_{14,1\sim 6} = 0$, $w_{14,31\sim 36} = 0$, $w_{14,49\sim 54} = 0$, $w_{14,55\sim 60} = 0$, $w_{14,61} = 1$ |
| $w_{15,1\sim 6} = 0$, $w_{15,25\sim 36} = 0$, $w_{15,55\sim 60} = 0$, $w_{15,61} = 1$, $w_{15,63\sim 64} = 0$ |

## 4 Conclusions

The SHA-3 Candidate algorithm Dynamic SHA2 family borrows the structure of SHA-2 family, but it uses the bits of message as parameters of the Boolean function $G$ and the rotation-shift function $ROTR$. This enables us to choose the number of shifts in the function $ROTR$ and the use of the function $G$ freely. In this paper, we present a near-collision attack on the compression functions of Dynamic SHA2-224/256 and SHA2-384/512 with complexity $2^{45}$ and $2^{75}$ respectively which is much higher than the ideal complexity of the near-collision attack.

## References

1. Z.Xu, Dynamic SHA2, NIST SHA-3 candidate, available from http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/ Dyamic-SHA2.zip.
2. National Institute of Standards and Technology (NIST). FIPS- 180-2: Secure Hash Standard, August 2002. Available online at http://www.itl.nist.gov/fipspubs/.
3. X.Y.Wang, H.B.Yu, How to Break MD5 and Other Hash Functions, Eurocrypt'05, LNCS 3494, pp.19-35.
4. X.Y.Wang, Y.L.Yin, H.B.Yu, Finding collisions on the Full SHA-1, Crypto'05, LNCS 3621, pp.17-36.

**Table 5.** The compression function of the Dynamic SHA-224/256.

| | | |
|---|---|---|
| $t = 0$ | $T_1[32] = ROTR(((((((a_0 \oplus b_0) + c_0) \oplus d_0) + e_0) \oplus f_0) + g_0) \oplus h_0[32]), w_0 \wedge 31)$<br>$a_1 = T_1[32] + w_1[32]$<br>$b_1 = a_0$<br>$c_1 = b_0$<br>$d_1 = G(a_0, b_0, c_0, SHR^{30}(w_0)) + w_2$<br>$e_1 = ROTR(d_0, SHR^{10}(w_0) \wedge 31)$<br>$f_1 = e_0 + w_3$<br>$g_1 = ROTR(f_0, SHR^{5}(w_0) \wedge 31)$<br>$h_1 = g_0$ | $w_{0,1\sim5} = 0$ |
| | $T_2 = ROTR(((((((a_1 \oplus b_1) + c_1) \oplus d_1) + e_1) \oplus f_1) + g_1) \oplus h_1), SHR^{15} w_0 \wedge 31)$<br>$a_2 = T_2 + w_4$<br>$b_2 = a_1$<br>$c_2 = b_1 + w_0$<br>$d_2 = G(a_1, b_1, c_1, 0) + w_5$<br>$e_2 = ROTR(d_1, SHR^{25}(w_0) \wedge 31)$<br>$f_2 = e_1 + w_6$<br>$g_2 = ROTR(f_1, SHR^{20}(w_0) \wedge 31)$<br>$h_2 = g_1 + w_7$ | |
| | $T_3 = ROTR(((((((a_2 \oplus b_2) + c_2) \oplus d_2) + e_2) \oplus f_2) + g_2) \oplus h_2), w_8 \wedge 31)$<br>$a_3 = T_3 + w_9$<br>$b_3 = a_2$<br>$c_3 = b_2$<br>$d_3 = G(a_2, b_2, c_2, SHR^{30}(w_8)) + w_{10}$<br>$e_3 = ROTR(d_2, SHR^{10}(w_8) \wedge 31)$<br>$f_3 = e_2 + w_{11}$<br>$g_3 = ROTR(f_2, SHR^{5}(w_8) \wedge 31)$<br>$h_3 = g_2$ | |
| | $T_4 = ROTR(((((((a_3 \oplus b_3) + c_3) \oplus d_3) + e_3) \oplus f_3) + g_3) \oplus h_3), SHR^{15}(w_8) \wedge 31)$<br>$a_4 = T_4 + w_{12}$<br>$b_4 = a_3$<br>$c_4 = b_3 + w_8$<br>$d_4 = G(a_3, b_3, c_3, 0) + w_{13}$<br>$e_4 = ROTR(d_3, SHR^{25}(w_8) \wedge 31)$<br>$f_4 = e_3 + w_{14}$<br>$g_4 = ROTR(f_3, SHR^{20}(w_8) \wedge 31)$<br>$h_4 = g_3 + w_{15}$ | |
| $t = 1$ | $T_5 = ROTR(((((((a_4 \oplus b_4) + c_4) \oplus d_4) + e_4) \oplus f_4) + g_4) \oplus h_4), w_1[32] \wedge 31)$<br>$a_5 = T_5 + w_2$<br>$b_5 = a_4$<br>$c_5 = b_4$<br>$d_5 = G(a_4, b_4, c_4, SHR^{30}(w_1[32])) + w_3$<br>$e_5 = ROTR(d_4, SHR^{10}(w_1[32]) \wedge 31)$<br>$f_5 = e_4 + w_4$<br>$g_5 = ROTR(f_4, SHR^{5}(w_1[32]) \wedge 31)$<br>$h_5 = g_4$ | $Pr(\Delta d_5 = 0) = 2^{-32}$<br>$w_{1,31} = 1$ |
| | $T_6 = ROTR(((((((a_5 \oplus b_5) + c_5) \oplus d_5) + e_5) \oplus f_5) + g_5) \oplus h_5), SHR^{15}(w_1[32]) \wedge 31)$<br>$a_6 = T_6 + w_5$<br>$b_6 = a_5$<br>$c_6[32] = b_5 + w_1[32]$<br>$d_6 = G(a_5, b_5, c_5, 1) + w_6$<br>$e_6 = ROTR(d_5, SHR^{25}(w_1[32]) \wedge 31)$<br>$f_6 = e_5 + w_7$<br>$g_6 = ROTR(f_5, SHR^{20}(w_1[32]) \wedge 31)$<br>$h_6 = g_5 + w_0$ | |
| | $T_7[32] = ROTR(((((((a_6 \oplus b_6) + c_6[32]) \oplus d_6) + e_6) \oplus f_6) + g_6) \oplus h_6), w_9 \wedge 31)$<br>$a_7[32] = T_7[32] + w_{10}$<br>$b_7 = a_6$<br>$c_7 = b_6$<br>$d_7[32] = G(a_6, b_6, c_6[32], SHR^{30}(w_9)) + w_{11}$<br>$e_7 = ROTR(d_6, SHR^{10}(w_9) \wedge 31)$<br>$f_7 = e_6 + w_{12}$<br>$g_7 = ROTR(f_6, SHR^{5}(w_9) \wedge 31)$<br>$h_7 = g_6$ | $w_{9,1\sim5} = 0$ |
| | $T_8 = ROTR(((((((a_7[32] \oplus b_7) + c_7) \oplus d_7[32]) + e_7) \oplus f_7) + g_7) \oplus h_7), SHR^{15}(w_9) \wedge 31)$<br>$a_8 = T_8 + w_{13}$<br>$b_8[32] = a_7[32]$<br>$c_8 = b_7 + w_9$<br>$d_8 = G(a_7[32], b_7, c_7, 1) + w_{14}$<br>$e_8[32] = ROTR(d_7[32], SHR^{25}(w_9) \wedge 31)$<br>$f_8 = e_7 + w_{15}$<br>$g_8 = ROTR(f_7, SHR^{20}(w_9) \wedge 31)$<br>$h_8 = g_7 + w_8$ | $b_{7,32} = 0$<br>$w_{9,26\sim30} = 0$ |

| | | |
|---|---|---|
| $t=2$ | $T_9 = ROTR((((((((a_8 \oplus b_8[32]) + c_8) \oplus d_8) + e_8[32]) \oplus f_8) + g_8) \oplus h_8), w_2 \wedge 31)$<br>$a_9 = T_9 + w_3$<br>$b_9 = a_8$<br>$c_9[32] = b_8[32]$<br>$d_9 = G(a_8, b_8[32], c_8, SHR^{30}(w_2)) + w_4$<br>$e_9 = ROTR(d_8, SHR^{10}(w_2) \wedge 31)$<br>$f_9[32] = e_8[32] + w_5$<br>$g_9 = ROTR(f_8, SHR^5(w_2) \wedge 31)$<br>$h_9 = g_8$ | $w_{2,31} = 1$<br>$w_{2,32} = 0$<br>$a_{8,32} = 0$ |
| | $T_{10} = ROTR((((((((a_9 \oplus b_9) + c_9[32]) \oplus d_9) + e_9) \oplus f_9[32]) + g_9) \oplus h_9), SHR^{15}(w_2) \wedge 31) + w_6$<br>$a_{10} = T_{10} + w_6$<br>$b_{10} = a_9$<br>$c_{10} = b_9 + w_2$<br>$d_{10}[32] = G(a_9, b_9, c_9[32], 2) + w_7$<br>$e_{10} = ROTR(d_9, SHR^{25}(w_2) \wedge 31)$<br>$f_{10} = e_9 + w_0$<br>$g_{10}[32] = ROTR(f_9[32], SHR^{20}(w_2) \wedge 31)$<br>$h_{10}[32] = g_9 + w_1[32]$ | $w_{2,21\sim 25} = 0$ |
| | $T_{11}[32] = ROTR((((((((a_{10} \oplus b_{10}) + c_{10}) \oplus d_{10}[32]) + e_{10}) \oplus f_{10}) + g_{10}[32]) \oplus h_{10}[32]), w_{10} \wedge 31)$<br>$a_{11}[32] = T_{11}[32] + w_{11}$<br>$b_{11} = a_{10}$<br>$c_{11} = b_{10}$<br>$d_{11} = G(a_{10}, b_{10}, c_{10}, SHR^{30}(w_{10})) + w_{12}$<br>$e_{11}[32] = ROTR(d_{10}[32], SHR^{10}(w_{10}) \wedge 31)$<br>$f_{11} = e_{10} + w_{13}$<br>$g_{11} = ROTR(f_{10}, SHR^5(w_{10}) \wedge 31)$<br>$h_{11}[32] = g_{10}[32]$ | $w_{10,1\sim 5} = 0$<br>$w_{10,11\sim 15} = 0$ |
| | $T_{12}[32] = ROTR((((((((a_{11}[32] \oplus b_{11}) + c_{11}) \oplus d_{11}) + e_{11}[32]) \oplus f_{11}) + g_{11}) \oplus h_{11}[32]), SHR^{15}(w_{10}) \wedge 31)$<br>$a_{12}[32] = T_{12} + w_{14}$<br>$b_{12}[32] = a_{11}[32]$<br>$c_{12} = b_{11} + w_{10}$<br>$d_{12} = G(a_{11}[32], b_{11}, c_{11}, 2) + w_{15}$<br>$e_{12} = ROTR(d_{11}, SHR^{25}(w_{10}) \wedge 31)$<br>$f_{12}[32] = e_{11}[32] + w_8$<br>$g_{12} = ROTR(f_{11}, SHR^{20}(w_{10}) \wedge 31)$<br>$h_{12} = g_{11} + w_9$ | $w_{10,16\sim 20} = 0$<br>$b_{11,32} = 0$ |
| $t=3$ | $T_{13}[32] = ROTR((((((((a_{12}[32] \oplus b_{12}[32]) + c_{12}) \oplus d_{12}) + e_{12}) \oplus f_{12}[32]) + g_{12}) \oplus h_{12}), w_3 \wedge 31)$<br>$a_{13}[32] = T_{13}[32] + w_4$<br>$b_{13}[32] = a_{12}[32]$<br>$c_{13}[32] = b_{12}[32]$<br>$d_{13} = G(a_{12}[32], b_{12}[32], c_{12}, SHR^{30}(w_3)) + w_5$<br>$e_{13} = ROTR(d_{12}, SHR^{10}(w_3) \wedge 31)$<br>$f_{13} = e_{12} + w_6$<br>$g_{13}[32] = ROTR(f_{12}[32], SHR^5(w_3) \wedge 31)$<br>$h_{13} = g_{12}$ | $w_{3,1\sim 5} = 0$<br>$w_{3,31\sim 32} = 0$<br>$w_{3,5\sim 10} = 0$ |
| | $T_{14} = ROTR((((((((a_{13}[32] \oplus b_{13}[32]) + c_{13}[32]) \oplus d_{13}) + e_{13}) \oplus f_{13}) + g_{13}[32]) \oplus h_{13}), SHR^{15}(w_3) \wedge 31)$<br>$a_{14} = T_{14} + w_7$<br>$b_{14}[32] = a_{13}[32]$<br>$c_{14}[32] = b_{13}[32] + w_3$<br>$d_{14} = G(a_{13}[32], b_{13}[32], c_{13}[32], 3) + w_0$<br>$e_{14} = ROTR(d_{13}, SHR^{25}(w_3) \wedge 31)$<br>$f_{14}[32] = e_{13} + w_1[32]$<br>$g_{14} = ROTR(f_{13}, SHR^{20}(w_3) \wedge 31)$<br>$h_{14}[32] = g_{13}[32] + w_2$ | $a_{13,32} = b_{13,32} + 1$ |
| | $T_{15} = ROTR((((((((a_{14} \oplus b_{14}[32]) + c_{14}) \oplus d_{14}) + e_{14}) \oplus f_{14}[32]) + g_{14}) \oplus h_{14}[32]), w_{11} \wedge 31)$<br>$a_{15} = T_{15} + w_{12}$<br>$b_{15} = a_{14}$<br>$c_{15}[32] = b_{14}[32]$<br>$d_{15} = G(a_{14}, b_{14}[32], c_{14}[32], SHR^{30}(w_{11})) + w_{13}$<br>$e_{15} = ROTR(d_{14}, SHR^{10}(w_{11}) \wedge 31)$<br>$f_{15} = e_{14} + w_{14}$<br>$g_{15}[32] = ROTR(f_{14}[32], SHR^5(w_{11}) \wedge 31)$<br>$h_{15} = g_{14}$ | $w_{11,31\sim 32} = 0$<br>$w_{11,5\sim 10} = 0$ |
| | $T_{16} = ROTR((((((((a_{15} \oplus b_{15}) + c_{15}[32]) \oplus d_{15}) + e_{15}) \oplus f_{15}) + g_{15}[32]) \oplus h_{15}), SHR^{15}(w_{11}) \wedge 31)$<br>$a_{16} = T_{16} + w_{15}$<br>$b_{16} = a_{15}$<br>$c_{16} = b_{15} + w_{11}$<br>$d_{16}[32] = G(a_{15}, b_{15}, c_{15}[32], 2) + w_8$<br>$e_{16} = ROTR(d_{15}, SHR^{25}(w_{11}) \wedge 31)$<br>$f_{16} = e_{15} + w_9$<br>$g_{16} = ROTR(f_{15}, SHR^{20}(w_{11}) \wedge 31)$<br>$h_{16}[32] = g_{15}[32] + w_{10}$ | |

| | | |
|---|---|---|
| $t = 4$ | $T_{17} = ROTR((((((((a_{16} \oplus b_{16}) + c_{16}) \oplus d_{16}[32]) + e_{16}) \oplus f_{16}) + g_{16}) \oplus h_{16}[32]), w_4 \wedge 31)$<br>$a_{17} = T_{17} + w_5$<br>$b_{17} = a_{16}$<br>$c_{17} = b_{16}$<br>$d_{17} = G(a_{16}, b_{16}, c_{16}, SHR^{30}(w_4)) + w_6$<br>$e_{17}[32] = ROTR(d_{16}[32], SHR^{10}(w_4) \wedge 31)$<br>$f_{17} = e_{16} + w_7$<br>$g_{17} = ROTR(f_{16}, SHR^5(w_4) \wedge 31)$<br>$h_{17} = g_{16}$ | $w_{4,11\sim15} = 0$ |
| | $T_{18}[32] = ROTR((((((((a_{17} \oplus b_{17}) + c_{17}) \oplus d_{17}) + e_{17}[32]) \oplus f_{17}) + g_{17}) \oplus h_{17}), SHR^{15}(w_4) \wedge 31)$<br>$a_{18}[32] = T_{18}[32] + w_0$<br>$b_{18} = a_{17}$<br>$c_{18} = b_{17} + w_4$<br>$d_{18}[32] = G(a_{17}, b_{17}, c_{17}, 0) + w_1[32]$<br>$e_{18} = ROTR(d_{17}, SHR^{25}(w_4) \wedge 31)$<br>$f_{18}[32] = e_{17}[32] + w_2$<br>$g_{18} = ROTR(f_{17}, SHR^{20}(w_4) \wedge 31)$<br>$h_{18} = g_{17} + w_3$ | $w_{4,16\sim20} = 0$ |
| | $T_{19}[32] = ROTR((((((((a_{18}[32] \oplus b_{18}) + c_{18}) \oplus d_{18}[32]) + e_{18}) \oplus f_{18}[32]) + g_{18}) \oplus h_{18}), w_{12} \wedge 31)$<br>$a_{19}[32] = T_{19}[32] + w_{13}$<br>$b_{19}[32] = a_{18}[32]$<br>$c_{19} = b_{18}$<br>$d_{19} = G(a_{18}[32], b_{18}, c_{18}, SHR^{30}(w_{12})) + w_{14}$<br>$e_{19}[32] = ROTR(d_{18}[32], SHR^{10}(w_{12}) \wedge 31)$<br>$f_{19} = e_{18} + w_{15}$<br>$g_{19}[32] = ROTR(f_{18}[32], SHR^5(w_{12}) \wedge 31)$<br>$h_{19} = g_{18}$ | $w_{12,1\sim5} = 0$<br>$w_{12,31} = 1$<br>$b_{18,32} = 0$<br>$w_{12,11\sim15} = 0$<br>$w_{12,6\sim10} = 0$ |
| | $T_{20} = ROTR((((((((a_{19}[32] \oplus b_{19}[32]) + c_{19}) \oplus d_{19}) + e_{19}[32]) \oplus f_{19}) + g_{19}[32]) \oplus h_{19}), SHR^{15}(w_{12}) \wedge 31)$<br>$a_{20} = T_{20} + w_8$<br>$b_{20}[32] = a_{19}[32]$<br>$c_{20}[32] = b_{19}[32] + w_{12}$<br>$d_{20} = G(a_{19}[32], b_{19}[32], c_{19}, 0) + w_9$<br>$e_{20} = ROTR(d_{19}, SHR^{25}(w_{12}) \wedge 31)$<br>$f_{20}[32] = e_{19}[32] + w_{10}$<br>$g_{20} = ROTR(f_{19}, SHR^{20}(w_{12}) \wedge 31)$<br>$h_{20}[32] = g_{19}[32] + w_{11}$ | |
| $t = 5$ | $T_{21} = ROTR((((((((a_{20} \oplus b_{20}[32]) + c_{20}[32]) \oplus d_{20}) + e_{20}) \oplus f_{20}[32]) + g_{20}) \oplus h_{20}[32]), w_5 \wedge 31)$<br>$a_{21} = T_{21} + w_6$<br>$b_{21} = a_{20}$<br>$c_{21}[32] = b_{20}[32]$<br>$d_{21} = G(a_{20}, b_{20}[32], c_{20}[32], SHR^{30}(w_5)) + w_7$<br>$e_{21} = ROTR(d_{20}, SHR^{10}(w_5) \wedge 31)$<br>$f_{21} = e_{20} + w_0$<br>$g_{21}[32] = ROTR(f_{20}[32], SHR^5(w_5) \wedge 31)$<br>$h_{21} = g_{20}$ | $w_{5,31\sim32} = 0$<br>$w_{5,6\sim10} = 0$ |
| | $T_{22} = ROTR((((((((a_{21} \oplus b_{21}) + c_{21}[32]) \oplus d_{21}) + e_{21}) \oplus f_{21}) + g_{21}[32]) \oplus h_{21}), SHR^{15}(w_5) \wedge 31)$<br>$a_{22}[32] = T_{22} + w_1[32]$<br>$b_{22} = a_{21}$<br>$c_{22} = b_{21} + w_5$<br>$d_{22}[32] = G(a_{21}, b_{21}, c_{21}[32], 1) + w_2$<br>$e_{22} = ROTR(d_{21}, SHR^{25}(w_3) \wedge 31)$<br>$f_{22} = e_{21} + w_3$<br>$g_{22} = ROTR(f_{21}, SHR^{20}(w_5) \wedge 31)$<br>$h_{22}[32] = g_{21}[32] + w_4$ | |
| | $T_{23}[32] = ROTR((((((((a_{22}[32] \oplus b_{22}) + c_{22}) \oplus d_{22}[32]) + e_{22}) \oplus f_{22}) + g_{22}) \oplus h_{22}[32]), w_{13} \wedge 31)$<br>$a_{23}[32] = T_{23} + w_{14}$<br>$b_{23}[32] = a_{22}[32]$<br>$c_{23} = b_{22}$<br>$d_{23} = G(a_{22}[32], b_{22}, c_{22}, SHR^{30}(w_{13})) + w_{15}$<br>$e_{23}[32] = ROTR(d_{22}[32], SHR^{10}(w_{13}) \wedge 31)$<br>$f_{23} = e_{22} + w_8$<br>$g_{23} = ROTR(f_{22}, SHR^5(w_{13}) \wedge 31)$<br>$h_{23} = g_{22}$ | $w_{13,1\sim5} = 0$<br>$w_{13,31} = 1$<br>$b_{22,32} = 0$<br>$w_{13,11\sim15} = 0$ |
| | $T_{24}[32] = ROTR((((((((a_{23}[32] \oplus b_{23}[32]) + c_{23}) \oplus d_{23}) + e_{23}[32]) \oplus f_{23}) + g_{23}) \oplus h_{23}), SHR^{15}(w_{13}) \wedge 31)$<br>$a_{24}[32] = T_{24}[32] + w_9$<br>$b_{24}[32] = a_{23}[32]$<br>$c_{24}[32] = b_{23}[32] + w_{13}$<br>$d_{24} = G(a_{23}[32], b_{23}[32], c_{23}, 1) + w_{10}$<br>$e_{24} = ROTR(d_{23}, SHR^{25}(w_{13}) \wedge 31)$<br>$f_{24}[32] = e_{23}[32] + w_{11}$<br>$g_{24} = ROTR(f_{23}, SHR^{20}(w_{13}) \wedge 31)$<br>$h_{24} = g_{23} + w_{12}$ | $w_{13,16\sim20} = 0$<br>$a_{23,32} = b_{23,32} + 1$ |

| | | |
|---|---|---|
| $t=6$ | $T_{25}=ROTR(((((((((a_{24}[32]\oplus b_{24}[32])+c_{24}[32])\oplus d_{24})+e_{24})\oplus f_{24}[32])+g_{24})\oplus h_{24}), w_6\wedge 31)$<br>$a_{25}=T_{25}+w_7$<br>$b_{25}[32]=a_{24}[32]$<br>$c_{25}[32]=b_{24}[32]$<br>$d_{25}=G(a_{24}[32], b_{24}[32], c_{24}[32], SHR^{30}(w_6))+w_0$<br>$e_{25}=ROTR(d_{24}, SHR^{10}(w_6)\wedge 31)$<br>$f_{25}[32]=e_{24}+w_1[32]$<br>$g_{25}[32]=ROTR(f_{24}[32], SHR^{5}(w_6)\wedge 31)$<br>$h_{25}=g_{24}$ | $w_{6,31}=1$<br>$a_{24,32}=b_{24,32}$<br>$w_{6,6\sim 10}=0$ |
| | $T_{26}=ROTR(((((((((a_{25}\oplus b_{25}[32])+c_{25}[32])\oplus d_{25})+e_{25})\oplus f_{25}[32])+g_{25}[32])\oplus h_{25}), SHR^{15}(w_6)\wedge 31)$<br>$a_{26}=T_{26}+w_2$<br>$b_{26}=a_{25}$<br>$c_{26}[32]=b_{25}[32]+w_6$<br>$d_{26}=G(a_{25}, b_{25}[32], c_{25}[32], 2)+w_3$<br>$e_{26}=ROTR(d_{25}, SHR^{25}(w_6)\wedge 31)$<br>$f_{26}=e_{25}+w_4$<br>$g_{26}[32]=ROTR(f_{25}[32], SHR^{20}(w_6)\wedge 31)$<br>$h_{26}[32]=g_{25}[32]+w_5$ | $a_{25,32}=1$<br>$w_{6,21\sim 25}=0$ |
| | $T_{27}[32]=ROTR(((((((((a_{26}\oplus b_{26})+c_{26}[32])\oplus d_{26})+e_{26})\oplus f_{26})+g_{26}[32])\oplus h_{26}[32]), w_{14}\wedge 31)$<br>$a_{27}=T_{27}[32]+w_{15}$<br>$b_{27}=a_{26}$<br>$c_{27}=b_{26}$<br>$d_{27}[32]=G(a_{26}, b_{26}, c_{26}[32], SHR^{30}(w_{14}))+w_8$<br>$e_{27}=ROTR(d_{26}, SHR^{10}(w_{14})\wedge 31)$<br>$f_{27}=e_{26}+w_9$<br>$g_{27}=ROTR(f_{26}, SHR^{5}(w_{14})\wedge 31)$<br>$h_{27}[32]=g_{26}[32]$ | $w_{14,1\sim 5}=0$ |
| | $T_{28}[32]=ROTR(((((((((a_{27}[32]\oplus b_{27})+c_{27})\oplus d_{27}[32])+e_{27})\oplus f_{27})+g_{27})\oplus h_{27}[32]), SHR^{15}(w_{14})\wedge 31)+w_{10}$<br>$a_{28}[32]=T_{28}[32]+w_{10}$<br>$b_{28}[32]=a_{27}[32]$<br>$c_{28}=b_{27}+w_{14}$<br>$d_{28}=G(a_{27}[32], b_{27}, c_{27}, 2)+w_{11}$<br>$e_{28}[32]=ROTR(d_{27}[32], SHR^{25}(w_{14})\wedge 31)$<br>$f_{28}=e_{27}+w_{12}$<br>$g_{28}=ROTR(f_{27}, SHR^{20}(w_{14})\wedge 31)$<br>$h_{28}=g_{27}+w_{13}$ | $w_{14,16\sim 20}=0$<br>$b_{27,32}=1$<br>$w_{14,26\sim 30}=0$ |
| $t=7$ | $T_{29}[32]=ROTR(((((((((a_{28}[32]\oplus b_{28}[32])+c_{28})\oplus d_{28})+e_{28}[32])\oplus f_{28})+g_{28})\oplus h_{28}), w_7\wedge 31)$<br>$a_{29}[32]=T_{29}[32]+w_0$<br>$b_{29}[32]=a_{28}[32]$<br>$c_{29}[32]=b_{28}[32]$<br>$d_{29}=G(a_{28}[32], b_{28}[32], c_{28}, SHR^{30}(w_7))+w_1[32]$<br>$e_{29}=ROTR(d_{28}, SHR^{10}(w_7)\wedge 31)$<br>$f_{29}[32]=e_{28}[32]+w_2$<br>$g_{29}=ROTR(f_{28}, SHR^{5}(w_7)\wedge 31)$<br>$h_{29}=g_{28}$ | $w_{7,1\sim 5}=0$<br>$w_{7,31}=1$<br>$w_{7,32}=0$<br>$b_{28,32}=a_{28,32}$ |
| | $T_{30}=ROTR(((((((((a_{29}[32]\oplus b_{29}[32])+c_{29}[32])\oplus d_{29})+e_{29})\oplus f_{29}[32])+g_{29})\oplus h_{29}), SHR^{15}(w_7)\wedge 31)$<br>$a_{30}[32]=T_{30}[32]+w_3$<br>$b_{30}[32]=a_{29}[32]$<br>$c_{30}[32]=b_{29}[32]+w_7$<br>$d_{30}=G(a_{29}[32], b_{29}[32], c_{29}[32], 3)+w_4$<br>$e_{30}=ROTR(d_{29}, SHR^{25}(w_7)\wedge 31)$<br>$f_{30}=e_{29}+w_5$<br>$g_{30}[32]=ROTR(f_{29}[32], SHR^{20}(w_7)\wedge 31)$<br>$h_{30}=g_{29}+w_6$ | $a_{29,32}=b_{29,32}+1$<br>$w_{7,21\sim 25}=0$ |
| | $T_{31}[32]=ROTR(((((((((a_{30}\oplus b_{30}[32])+c_{30}[32])\oplus d_{30})+e_{30})\oplus f_{30})+g_{30}[32])\oplus h_{30}), w_{15}\wedge 31)$<br>$a_{31}[32]=T_{31}[32]+w_8$<br>$b_{31}=a_{30}$<br>$c_{31}[32]=b_{30}[32]$<br>$d_{31}=G(a_{30}, b_{30}[32], c_{30}[32], SHR^{30}(w_{15}))+w_9$<br>$e_{31}=ROTR(d_{30}, SHR^{10}(w_{15})\wedge 31)$<br>$f_{31}=e_{30}+w_{10}$<br>$g_{31}=ROTR(f_{30}, SHR^{5}(w_{15})\wedge 31)$<br>$h_{31}[32]=g_{30}[32]$ | $w_{15,1\sim 5}=0$<br>$w_{15,31\sim 32}=0$ |
| | $T_{32}[32]=ROTR(((((((((a_{31}[32]\oplus b_{31})+c_{31}[32])\oplus d_{31})+e_{31})\oplus f_{31})+g_{31})\oplus h_{31}[32]), SHR^{15}(w_{15})\wedge 31)$<br>$a_{32}[32]=T_{32}[32]+w_{11}+a_0$<br>$b_{32}[32]=a_{31}[32]+b_0$<br>$c_{32}=b_{31}+w_{15}+c_0$<br>$d_{32}=G(a_{31}[32], b_{31}, c_{31}[32], 3)+w_{12}+d_0$<br>$e_{32}=ROTR(d_{31}, SHR^{25}(w_{15})\wedge 31)+e_0$<br>$f_{32}=e_{31}+w_{13}+f_0$<br>$g_{32}=ROTR(f_{31}, SHR^{20}(w_{15})\wedge 31)+g_0$<br>$h_{32}[32]=g_{31}+w_{14}+h_0[32]$ | $w_{15,16\sim 20}=0$<br>$b_{31,32}=1$ |